UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

THOMAS BUCHANAN, on behalf of himself and all others similarly situated,	§	
Plaintiff,	§	
v.	§	Civil Case No. 3:17-cv-00728-D
SIRIUS XM RADIO, INC.	§	
Defendant.	§	

PLAINTIFF'S MOTION TO COMPEL
AND MOTION FOR PROTECTIVE ORDER

Thomas Buchanan ("Plaintiff" or "Mr. Buchanan"), individually, and on behalf of all others similarly situated, files this Motion to Compel and for a Protective Order, and in support thereof would shows as follows:

INTRODUCTION

Plaintiff brings this Telephone Consumer Protection Act ("TCPA"), 47 U.S.C. § 227 *et seq.*, class action against Defendant Sirius XM Radio, Inc. ("Sirius"), for illegal telemarketing calls to consumers' telephones. Although the TCPA grants an unqualified right for people registered to the National Do Not Call ("NDNC") Registry to avoid unwanted telemarketing calls, Sirius and its agents made telemarketing calls to persons registered on the NDNC Registry and failed to establish the required minimum procedures to stop calling people who requested that such calls end.

Production of call data sufficient to ascertain the proposed class is standard practice in TCPA class actions. *See, e.g., Ossola v. Am. Express Co.*, 2015 WL 5158712, at *7 (N.D. Ill.

2015) ("Call data is relevant, and thus produced as standard practice . . . in cases where the defendant is the alleged dialer."). Sirius has nonetheless refused such production unless Plaintiff agrees to costly and burdensome procedures to sequester the data with a third-party vendor and require Plaintiff's counsel, vendors and experts to personally indemnify Sirius if Sirius' data security procedures do not work. Sirius has not cited a single decision—in any court, anywhere—that imposed such procedures. Plaintiff respectfully requests that the Court overrule Sirius's objections and order a fully responsive production.

BACKGROUND

A. The Telephone Consumer Protection Act

Congress enacted the TCPA to prevent telemarketing calls by companies that escaped state invasion of privacy and nuisance statutes by operating interstate. *Mims v. Arrow Fin. Servs. LLC*, 132 S. Ct. 740, 745 (2012). Congress embedded the reasons for the TCPA into the statute itself with explicit Congressional Findings noting that "[u]nrestricted telemarketing . . . can be an intrusive invasion of privacy." 105 Stat. 2394, § 5 (notes following 47 U.S.C. § 227). "The TCPA is essentially a strict liability statute … [and] does not require any intent for liability except when awarding treble damages." *Alea London Ltd. v. Am. Home Servs., Inc.*, 638 F.3d 768, 776 (11th Cir. 2011) (citation omitted).

The TCPA prohibits sellers from making telephone solicitations to people who have registered their telephone numbers on the NDNC Registry. 47 U.S.C. § 227(c)(5); *Krakauer v. Dish Network L.L.C.*, 311 F.R.D. 384, 387 (M.D.N.C. 2015) (certifying a nationwide TCPA NDNC Registry class and a nationwide TCPA internal Do Not Call list class). The TCPA prohibits telemarketer calls to an NDNC registrant unless that registrant provides prior express written consent to receive the calls in a signed, written agreement. 47 C.F.R. § 64.1200(c)(2)(ii). To avoid

calling a number listed on the Registry, a telemarketer can easily and inexpensively "scrub" its call lists against the Registry database at least once every thirty-one days. *See* 16 C.F.R. § 310.4(b)(3)(iv).

The TCPA also prohibits *all* telemarketing calls "unless such [company] has instituted procedures for maintaining a list of persons who request not to receive telemarketing calls by or on behalf of that [company]." 47 C.F.R. § 64.1200(d). The "minimum standards" for these procedures include placing an individual's phone number on an internal do-not-call registry, to honor that request no later than thirty days of its receipt—and not calling that number again. 47 C.F.R. § 64.1200(d)(3). A company violates the TCPA when it "initiat[es a] phone call without having implemented the minimum procedures." *Wagner v. CLC Resorts & Developments, Inc.*, 32 F. Supp. 3d 1193, 1198 (M.D. Fla. 2014) (citations omitted).

Vicarious liability is well established under the TCPA for all calls "by ***or on behalf of*** the same entity in violation of the regulations." 47 U.S.C. § 227(c)(5) (emphasis added). Congress vested the Federal Communication Commission ("FCC") with authority to issue regulations implementing the TCPA. 47 U.S.C. § 227(b)(2). Under FCC regulations, vicarious liability may be based on the principles of apparent authority, actual authority, and ratification, or, under the express terms of §227(c), when unlawful calls are placed "on behalf of" the seller. *In re Joint Pet. Filed by Dish Network*, 28 FCC Rcd. 6574 (2013).[1] FCC rulings are binding on this Court because

[1] *See also In The Matter of Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991: Request of State Farm for Clarification and Declaratory Ruling,* 20 FCC Rcd 13664, 13666-13668 (FCC 2005) ("We take this opportunity to reiterate that a company on whose behalf a telephone solicitation is made bears the ultimate responsibility for any violation of our telemarketing rules and calls placed by a third party on behalf of the company are treated as if the company itself placed the call.").

the federal appellate courts have exclusive jurisdiction over challenges to FCC rulings. *See* 28 U.S.C. § 2342; *Mais v. Gulf Coast Collection Bureau, Inc.*, 768 F.3d 1110, 1119 (11th Cir. 2014).

B. Plaintiff's Class Action Complaint

Plaintiff alleges that Sirius, in violation of the TCPA, has engaged in a practice of making telemarketing calls to consumers on the NDNC Registry and of failing to implement the required minimum procedures to honor consumers' do-not-call requests. (Dkt. 1.)

In 2008, Mr. Buchanan listed his home telephone number on the NDNC. (Dkt. 1 at ¶ 31.)[2] Nonetheless, in 2016, Sirius began placing telemarketing sales calls to Mr. Buchanan's home. (*Id.* at ¶ 34.) Mr. Buchanan never provided prior express consent to Sirius to call his home. (*Id.* at ¶ 38.) On July 24, 2016, Mr. Buchanan sent a letter to the company requesting that it immediately stop making these unauthorized telemarketing calls to him, and place his number on Sirius' internal do-not-call registry. (*Id.* at ¶ 36.) Nevertheless, Sirius continued to call Mr. Buchanan's home. (*Id.* at ¶ 37.)

Mr. Buchanan seeks to represent a National Do Not Call Registry Class and an Internal Do Not Call Registry Class, as defined in the Class Action Complaint. (*Id.* at ¶¶ 39, 41.) The only way to ascertain the actual size of the classes, and to identify who should be included in the classes, is to review Sirius' call data. (*See id.* at ¶ 43.)

C. Status of Discovery

On August 8, 2017, Plaintiff served discovery requests seeking documents or ESI sufficient to ascertain the proposed classes. (Exs. 1 & 2.) Specifically, Plaintiff requested, *inter alia*, (1) data evidencing the number and identity of proposed class members to whom Sirius placed a call

[2] References to "Dkt" are to documents filed on the Court's ECF Docket in this action. References to "Ellzey Aff." are to the Affidavit of Jarret Ellzey, dated March 7, 2018 and filed here with. References to "Ex." are to the exhibits to the Ellzey Aff.

during the class period, (*id.* at Request Nos. 23-24), and (2) Sirius's internal do-not-call list. (*Id.* at Request No. 78.). Sirius objected to these requests. As detailed in the accompanying declaration of counsel, the parties met and conferred extensively regarding Sirius' objections and Plaintiff's need for these documents. (Ellzey Aff. at ¶¶ 11 - 30.)

On October 16, 2017, Sirius agreed to produce the call logs received from its vendors by providing a "file that will consist of all calls placed on its behalf by telemarketing vendors during the relevant class period. It will contain at least the telephone number called and the date and time of call." (Ex. 5.)

Sirius, however, declined to produce the name and address of the consumer called, or its internal do-not-call list, and stated that it would only produce the call logs if the parties agreed to Sirius' preferred protective order. Sirius's proposed protective order required stringent and overly burdensome digital data protection procedures, and "unlimited" *personal* indemnification to Sirius if its suggested digital data protection procedures fail and result in unauthorized access to the data. (Ex. 6 at p. 13 ¶ 7.3.) Sirius' proposal would require the following, among other things:

- Anyone receiving the call logs (the "Data Recipients") must "maintain appropriate security measures to protect the confidentiality of personally identifying information consistent with the applicable regulations of the Commonwealth of Massachusetts (201 CMR 17.00, et. Seq.), the regulations of California (Cal. Civ. Code §§ 56.06, 1785.11.2, 1798.29, 1798.82), and *all other states*." (Ex. 6 at p. 26 § 2 (emphasis added).)
- Data Recipients must keep the data "at a facility that maintains technical, organizational, administrative, and human resource security measures which utilize

ISO 27001 and 27002 as a reference to protect the security of" all Call Recipient Contact Information produced. (*Id.* at p. 27 § 5.)

- Data Recipients must encrypt the Call Recipient Contact Information at all times, and the encryption must meet strict standards established in the Data Security Acknowledgment. (*Id.* at p. 27 § 6.)
- In the event of any unauthorized access to the data, Data Recipients must personally agree to pay, *inter alia,* to conduct an investigation approved by Sirius and to notify anyone who's information was affected along with the relevant credit bureaus, and other persons or entities that Sirius deems appropriate. (*Id.* at p. 27 § 4.)
- Data Recipients must personally agree to unlimited indemnification of Sirius, specifically that the Data Recipients:

> shall indemnify, defend and hold harmless [Sirius], its affiliates, and their respective employees, officers and directors against any and all third party claims and resulting damages, costs and other liabilities and expenses (including attorneys' fees) arising out of or related to: (i) any negligence or willful misconduct by [Plaintiff], its affiliates, its subcontractors, or their agents; (ii) a breach or alleged breach of any of its representations, warranties or obligations of this Agreement by [Plaintiff], its affiliates, its subcontractors, or their agents; (iii) any loss of Private Person Information by [Plaintiff], its affiliates, its contractors, or their agents; and (iv) any failure or alleged failure by [Plaintiff], its affiliates, its subcontractors, or their agents to comply with any applicable law, rule, and regulation with respect to its performance of this Agreement. (*Id.* at p. 28 § 7.)

Although Sirius' requirements were unduly burdensome, Plaintiff continued to meet and confer in good faith. (Ellzey Aff. at ¶¶ 22 - 29.) After a time consuming search, Plaintiff's counsel located only three vendors that provided sophisticated secure data room software with the capabilities to meet Sirius' data security requirements. (Ellzey Aff. at ¶ 27.) The first vendor charged $7,400 per month, a clearly unreasonable sum to protect non-sensitive information such

as names and contact information. (*Id.*) The second vendor charged $1,500 per month, still a burdensome amount, and stated that it could not meet all of the various security requirements. (*Id.*) The Third vendor charged less, but upon reviewing the Data Security Acknowledgment stated that the indemnification provisions were not reasonable under the circumstances and that it could not take on that type of potentially unlimited liability. (*Id.*)

Even though Plaintiff believed these expenses and the data security requirements were unduly burdensome, in hopes of reaching an agreement without resorting to the instant motion, Plaintiff told Sirius that he would be willing to incur the required fees to host the data securely, if Sirius would agree to certain changes to the Data Security Acknowledgment, including (1) identifying specifically which states' laws Plaintiff needed to comply with; (2) limiting the financial and logistical requirements that Plaintiff would need to meet in the event someone gained unauthorized access to the data; and (3) dropping the demand for indemnification. However, negotiations on this issue broke down after Sirius refused to withdraw these requirements. (Ellzey Aff. at ¶ 28, Ex. 7)

As this background makes clear, prior to making this motion, the parties made significant efforts to meet and confer to obtain the necessary documents without court action. Regrettably these efforts failed. Plaintiff now respectfully seeks an order compelling Sirius to produce documents relevant to Plaintiff's motion for class certification pursuant to a reasonable protective order.

LEGAL ANALYSIS

I. MOTION TO COMPEL DISCOVERY

A. Standard for a Motion to Compel Discovery

A "[c]ourt has broad discretion in determining the appropriate scope of discovery." *In re: DePuy Orthopaedics, Inc.*, No. 3:11-MD-2244-K, 2016 WL 6496462, at *2 (N.D. Tex. Jan. 6, 2016). In general, "[p]arties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense . . . ." Fed. R. Civ. P. 26(b)(1). What is relevant "encompasses any matter that bears on, or that reasonably could lead to other matter that could bear on, any issue that is or may be in the case." *Coughlin v. Lee*, 946 F.2d 1152, 1159 (5th Cir. 1991). "In the discovery context, [r]elevancy is broadly construed, and a request for discovery should be considered relevant if there is any possibility that the information sought may be relevant to the claim or defense of any party." *Moss v. Princip*, No. 3:14-CV-3088-BF, 2017 WL 2879694, at *1 (N.D. Tex. June 1, 2017) (internal quotations omitted); *Mateos v. Select Energy Servs., LLC*, No. SA-12-CA-00529-DAE, 2014 WL 12588336, at *1 (W.D. Tex. Oct. 8, 2014) (same).

"Under Federal Rule of Civil Procedure 37, '[a] party seeking discovery may move for an order compelling an answer, designation, production, or inspection' when a party fails to respond to an interrogatory or produce requested documents." *Duarte v. St. Paul Fire & Marine Ins. Co.,* No. EP-14-CV-305-KC, 2015 WL 7709433, at *3 (W.D. Tex. Sept. 25, 2015) (*quoting* Fed. R. Civ. P. 37(a)(3)(B)(iii)-(iv)). The party making the motion must initially show that the information sought is relevant. *Moss v. Princip*, No. 3:14-CV-3088-BF, 2017 WL 2879694, at *1 (N.D. Tex. June 1, 2017). "Once the moving party establishes that the information and materials sought are within the scope of permissible discovery, the burden shifts to the nonmovant to show why the discovery is irrelevant, overly broad, unduly burdensome, or should not be permitted." *Id.*

B. Sirius Should be Compelled to Produce Its Call Log In the Manner it is Stored, and Including the Call Recipients' Phone Number, Name and Address

In TCPA class actions, pre-class-certification discovery of call data is relevant to Rule 23's requirements for class certification. Courts therefore routinely order production of call data sufficient to ascertain the proposed class in TCPA cases. For example, in *City Select Auto Sales Inc. v. BMW Bank of N. Am. Inc.*, 867 F.3d 434 (3d Cir. 2017), the TCPA plaintiff sought production of the phone number of each person in the proposed class. The magistrate judge denied that motion. *Id.* at 437 n.1. Following a ruling on class certification, the plaintiff appealed. The Third Circuit found that Rule 23's ascertainability standard requires a plaintiff to show that "(1) the class is defined with reference to objective criteria; and (2) there is a reliable and administratively feasible mechanism for determining whether putative class members fall within the class definition." *Id.* at 439 (internal quotations and citations omitted). The *City Select* court held: "because the [defendant's] database was not produced during discovery, plaintiff was denied the opportunity to demonstrate whether a reliable, administratively feasible method of ascertaining the class exists based, in whole or in part, on that database." *Id.* at 440-41. The court vacated and remanded to the district court with instructions that the defendant's records be produced. *Id.* at 443.

Courts throughout the country have likewise found that production of call data sufficient to ascertain the proposed class is "standard practice" in TCPA class actions.[3]

[3] *See, e.g.*, *Mbazomo v. ETourandTravel, Inc.*, No. 2:16-CV-02229-SB, 2017 WL 2346981, at *5 (E.D. Cal. May 30, 2017) (call logs and dialing lists relevant to numerosity and commonality); *Ossola v. Am. Express Co.,* 2015 WL 5158712, at *7 (N.D. Ill. 2015) ("Call data is relevant, and

Such data is relevant because it speaks to issues upon which a district court must pass in deciding whether a suit should proceed as a class action under Rule 23, such as numerosity, ascertainability, commonality, and predominance.

Here, Sirius admits that it maintains responsive call data along with data concerning the name and address of the individuals called. (Ellzey Aff. at ¶ 16; Ex. 4.) Sirius articulates no specific cost or burden associated with searching for and producing its electronic records. Sirius should be compelled to produce those records. *See City Select Auto Sales*, 867 F.3d at 441-42 (permitting the ascertainability standard to be addressed, among other ways, through "databases," "other available records," or "other reliable and administratively feasible means").

C. Sirius Should be Compelled to Produce Its Internal Do-Not-Call List In the Manner it is Stored

Production of an internal do-not call list is routine and non-controversial. *See, e.g.*, *Krakauer v. Dish Network L.L.C.,* 311 F.R.D. 384, 391 (M.D.N.C. 2015) (certifying class and

---

thus produced as standard practice . . . in cases where the defendant is the alleged dialer."); *Knutson v. Schwan's Home Serv., Inc.*, 2013 WL 3746118, at *4 (S.D. Cal. July 15, 2013) (ordering the production of a "dial list" consisting of everyone in the plaintiff's proposed class); *Gossett v. CMRE Fin. Servs.*, 142 F. Supp. 3d 1083, 1087 (S.D. Cal. 2015) (same); *Thrasher v CMRE Financial Services, Inc.*, 2015 U.S. Dist. LEXIS 34965 (S.D. Cal. March 13, 2015) (same); *Gusman v. Comcast Corp.*, 298 F.R.D. 592 (S.D. Cal. 2014) (same); *Webb v. Healthcare Revenue Recovery Grp. LLC*, 2014 WL 325132, at *2-3 (N.D. Cal. Jan. 29, 2014) (same); *Whiteamire Clinic, P.A. v. Quill Corp.*, 2013 WL 5348377, at *2 (N.D. Ill. 2013) (same); *Martin v. Bureau of Collection Recovery*, No. 10 C 7725, 2011 U.S. Dist. LEXIS 157579 at *8-*12 (N.D. Ill. June 13, 2011) (same); *Donnelly v. NCO Fin. Sys., Inc.,* 263 F.R.D. 500, 503-504 (N.D. Ill. 2009) (same); *see also Gilman v. ER Solutions*, No. C11-0806-JCC, Order, Dkt. No. 67, at p.4 (W.D. Wash. Feb. 3, 2012) ("Class certification cannot fairly be evaluated without information on whether others received automated calls to which they did not expressly consent, and Plaintiffs have no way to gather this information aside from the discovery requests [defendant] opposes.").

noting that the defendant produced data files containing its internal do-not-call list); *see also Buja v. Novation Capital, LLC*, No. 15-CV-81002, 2016 WL 9026498, at *3 (S.D. Fla. Dec. 27, 2016) ("Defendants have already provided Plaintiff with their internal do-not-call list"). Since Sirius maintains responsive data and would suffer no specific cost or burden from producing it, Sirius should be compelled to produce those records.

II. MOTION FOR A PROTECTIVE ORDER

Since Sirius is willing and able to produce responsive data, the only question is whether Plaintiff should be subjected to the onerous protective order proposed by Sirius. As an initial matter, Plaintiff has no objection to a protective order that protects confidential documents Sirius has produced or will produce. Plaintiff can even consent to Sirius' demand to designate certain documents as being for "Attorney's Eyes Only."

Nevertheless, Plaintiff cannot agree to expensive and unnecessary data security procedures or to "unlimited" personal indemnification of Sirius if Sirius' procedures do not work. First, heightened data security procedures are not necessary to protect non-private information such as the call recipient's names, addresses and phone numbers. Second, personal indemnification would be unduly burdensome and is a naked attempt to dissuade Plaintiff from enforcing his and similarity situated class members rights under the TCPA. As such, Plaintiff asks that this Court enter a protective order in the form attached as Exhibit 9 to the Ellzey Affidavit, without the Data Security Acknowledgment.

A. Standard for a Protective Order

"The court may, for good cause, issue an order to protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense, including . . . requiring that a trade secret or other confidential research, development, or commercial information not be revealed or be

revealed only in a specified way." Fed. R. Civ. P. 26. To establish good cause, "[t]he movant bears the burden of showing that a protective order is necessary, 'which contemplates a particular and specific demonstration of fact as distinguished from stereotyped and conclusory statements.'" *Equal Empl. Opportunity Commn. v. BDO USA, L.L.P.*, 876 F.3d 690 (5th Cir. 2017) (quoting *In re Terra Int'l*, 134 F.3d 302, 306 (5th Cir. 1998) (internal quotations omitted)).

"When parties to an action agree on entry of a protective order but differ on the order's terms" as is the case here "the party seeking to limit discovery bears the burden of demonstrating that 'good cause' exists for the protection of that information." *Doc. Generation Corp. v. Allscripts, LLC*, No. CIV A 6:08-CV-479, 2009 WL 1766096, at *2 (E.D. Tex. June 23, 2009) (holding that the defendant had failed to meet its burden to entering a more restrictive protective order). Sirius is seeking a more restrictive version of the protective order by refusing to produce documents without the Data Security Acknowledgment, therefore, the burden is on it to show why there is good cause to enter such heightened data security and indemnification. *iLife Techs., Inc v. OnAsset Intelligence, Inc.*, No. 3:12-CV-05155-M-BK, 2013 WL 12126265, at *1 (N.D. Tex. Oct. 22, 2013).

"A protective order may be fashioned only after balancing the potential harm to the affected party and the need of the requesting party for the particular information." *Gutierrez v. Benavides*, 292 F.R.D. 401, 403 (S.D. Tex. 2013). Where one party is seeking a heightened level of protection, and the other party is opposing that heightened protection, Federal Courts in Texas Courts often look to several factors to determine if the heightened protection is warranted, including "the risk and potential danger of disclosure" and the "hardship and prejudice" imposed on the receiving party by the protections. *Merial Ltd. v. Virbac SA*, No. 4:10-CV-181-Y, 2010 WL 11534378, at *2 (N.D. Tex. June 10, 2010) (refusing to require for attorneys' eyes only protection); *ST Sales*

Tech Holdings, LLC v. Daimler Chrysler Co., LLC, CIV.A. 6:07-CV-346, 2008 WL 5634214, at *2 (E.D. Tex. Mar. 14, 2008).[4]

B. The Call Recipient Contact Information Does Not Warrant Heightened Data Security Procedures

The information that Sirius insists be protected by the heightened data security procedures includes "customer names, addresses, and/or telephone numbers." Therefore, the only information Plaintiff has requested as part of its class certification discovery that would be affected by the data security requirements are the names, addresses and phone numbers contained in either Sirius' marketing database and call logs or its internal do-not-call list (the "Call Recipient Contact Information "). A person's name, address and phone number are not private confidential pieces of information, as such, that information does not warrant the heightened data security procedures that Sirius seeks.

Plaintiff has *not* requested sensitive personal information, such as that recognized in Federal Rule 5.2 (*e.g.*, social security numbers, financial information, or birth years). Instead, Plaintiff is only seeking contact information. Courts inside and outside this Circuit have recognized that names and contact information do not present the same type of privacy concerns as more sensitive information. *E.g., S. Ave. Partners LP v. Blasnik*, 3:09-CV-0765-M-BK, 2013 WL 12224041, at *4 (N.D. Tex. June 21, 2013) (ordering disclosure during pre-certification discovery of the names and contact information for punitive class members, and noting that the

[4] The issue of whether heightened protection is necessary often arises in Texas Federal Courts in the context of patent cases where the question is whether in-house counsel or employees should be allowed access to the data being produced, as was the case in both *Merial Ltd.* and *ST Sales Tech Holdings, LLC*. As such, these courts also examined whether the person receiving the data was a decision maker at a competitor, thereby examining the competitive risk to production. Obviously, this factor is not relevant here because Plaintiff and his counsel are in no way competitors to Sirius, but the remaining two factors highlighted above provide useful guides for the analysis in this case.

court was less concerned with privacy issue for such information than for more sensitive information like medical records); *Thrasher v. CMRE Fin. Services, Inc.*, 14-CV-1540 BEN NLS, 2015 WL 1138469, at *3 (S.D. Cal. Mar. 13, 2015) (holding in a TCPA case that "[t]he disclosure of phone numbers and names does not constitute a serious invasion of privacy and is commonplace in class actions"); *Stemple v. QC Holdings, Inc.*, Civil No. 12-cv-1997, 2013 U.S. Dist. LEXIS 99582, at *10-13 (S.D. Cal. June 17, 2013) ("Disclosure of phone numbers and names does not constitute a serious invasion of privacy and is commonplace in class actions."); *see also Alvarez v. Hyatt Regency Long Beach*, No. CV 09-04791, 2010 U.S. Dist. LEXIS 99281, at *5 (C.D. Cal. Sept. 21, 2010) ("In the class action context, disclosure of names, addresses and telephone numbers is common practice.").

To the contrary, most people regularly provide their names, addresses and telephone numbers to third parties, and that information has traditionally been publicly disclosed in, *inter alia*, telephone books. As a result, individual's expectation of privacy in such information is very low. *See Thurby v. Encore Receivable Mgmt., Inc.*, 251 F.R.D. 620, 622 (D. Colo. 2008) (holding that personal contact information is not confidential because it is "regularly disclosed to friends, relatives, vendors, credit card companies, schools, children's sports teams, and the like."); *Plastic the Movie Ltd. v. John Doe Subscriber Assigned IP Address 24.0.105.163*, No. CIV. 15-2446 JHR/JS, 2015 WL 4715528, at *1 (D.N.J. Aug. 7, 2015) (holding that names, addresses and phone numbers are "not privileged or confidential" because people regularly provide such information to third parties and therefore "do not have a reasonable expectation of privacy" in such information (internal quotations omitted)).

In fact, the state level data security statues that Sirius cites to in the Data Security Acknowledgment *support* Plaintiff's argument because none consider contact information alone

to be private. 201 CMR 17.02 (defining personal information to only include data sets with both a Massachusetts' residents' names *and* either their social security number, driver's license number, or financial account numbers); Cal. Civ. Code § 1798.29(g) (defining personal information to only include data sets with both a person's name *and* either his/her security number, driver's license numbers, financial account numbers, medical information, health insurance information or license plate data automatically collected).[5]

As part of the negotiation process, Sirius' counsel stated that it was insisting on the heightened data security protections because they "are industry standards and consistent with Sirius' own internal standards, and Sirius has also agreed with at least some OEMs to maintain their customer information consistent with these standards." (Ex. 7.) However, here Plaintiff is not a participant in the industry, and is not seeking to use this information for commercial gain. Instead he is attempting to vindicate his rights, and those of others like him, that Congress recognized in the TCPA and that he has reason to believe Sirius has violated. For that reason, courts in this Circuit, all be it in other contexts, have already rejected the argument that a litigant should be required to comply with industry standard data security precautions. See *United States v. Ocwen Loan Servicing, LLC*, No. 4:12-CV-543, 2016 WL 278967, at *6 (E.D. Tex. Jan. 22, 2016) (refusing to issue a protective order requiring the Plaintiff to observe "the same privacy and

[5] Sirius' inclusion of these state level statutes in the Data Security Acknowledgment is both overly broad and impermissible vague. First, as noted above, neither of the two statutes cited in the Data Security Acknowledgment apply to the information at issue in this case. Second, the inclusion of the phrase "and all other states" is impermissibly vague and overly burdensome because without doing a 50-state survey it would be impossible for someone to be assured they are complying with all data security requirements in every state. Moreover, it does not account for when/if two state's data security requirements conflict. As a result, paragraph 2 of the Data Security Acknowledgment is too vague to allow in the Protective Order. *See Scott v. Schedler*, 826 F.3d 207, 213 (5th Cir. 2016) (holding that a district court order was too vague because it told the secretary of state to continue to enforce his "policies, procedures, and directives, as revised, relative to the implementation of the" voting rights act).

data security obligations imposed on Defendants" who were debt collectors, and to "[c]omply with Texas's information security requirements," because those requirements were specific to commercial actors in the industry).

As to Sirius' claim that it has obligations to third parties to maintain the information in accordance with these data security precautions, there is no reason why that requirement should transfer to Plaintiffs in these circumstances. Plaintiff asked Sirius to identify the specific language in its third-party agreements that it claimed required Plaintiff to adhere to this level of security, but Sirius has refused to provide that language. Furthermore, even if Sirius has contractual obligations to maintain certain levels of security, those agreements should not impede production. Instead, standard confidentiality provisions in Plaintiff's proposed protective order, such as designating documents as "Confidential," or as "Attorneys' Eyes Only" should be sufficient, combined with this court's order to produce that information, to satisfy such requirements. *See Nvision Biomedical Techs., LLC v. Jalex Med., LLC,* No. 5:15-CV-284 RP, 2016 WL 8285637, at *2 (W.D. Tex. Feb. 1, 2016) (ordering production of documents that were subject to a nondisclosure agreement with third parties and that "the existing Confidentiality and Protective Order . . . is sufficient to satisfy" any concerns over sensitive or proprietary information); *Tinkers & Chance v. Leapfrog Enterprises, Inc.,* No. CIV.A. 2:05-CV-349, 2006 WL 462601, at *2 (E.D. Tex. Feb. 23, 2006) (ordering "the production of all relevant documents and evidence, without regard to any private non-disclosure agreements" and that such documents should be marked confidential under the parties' protective order). A party should not be allowed to enter into private contractual relations that have the effect of later impeding justice by making production of necessary information impractical or impossible.

C. Plaintiff Should Not Be Required To Indemnify Defendant

In addition to the expensive security procedures demanded by Sirius, it has also insisted that all Data Recipients agree to *personally* indemnify Sirius in the event that the Call Recipient Contact Information is stolen or misused. (Ex. 6 at p. 28 ¶ 7.) The way Sirius has structured the indemnification, the Data Recipients could take all the security precautions Sirius demands, do nothing wrong, and still have the Call Recipient Contact Information stolen and thereby be personally liable to Sirius. *Id.*

For the reasons stated above, Plaintiff has a right under the Federal Rules to receive the Call Recipient Contact Information from Sirius. Also, as noted, the Call Recipient Contact Information is not sensitive private information, and as such, poses little risk to the call recipients if it is stolen by a hacker. Nevertheless, if the information is stolen, Sirius wants the Data Recipients to personally agree to pay, *inter alia*, for Sirius' "damages, costs and other liabilities and expenses (including attorneys' fees)," for "conducting the investigation" of any data theft, and for the cost of "notifying affected persons, credit bureaus, or other persons or entities deemed appropriate by" Sirius.[6] (Ex. 6 at pp. 27-28 ¶¶ 4, 7.) These are all costs that the Data Recipients would need to pay even if there was never any damage caused to the call recipients themselves. These costs could potentially be crippling for an individual Data Recipient.

[6] As part of negotiations, Sirius asserted that the notification requirements are required by law in several states. Sirius again did not specify which states it was referring to, but even assuming that is the case, if notification is required by state law, there is no reason to additionally require it here or to automatically place the burden of paying for such notices on the Data Recipients. *Hindle v. Natl. Bulk Carriers*, 18 F.R.D. 198, 199 (S.D.N.Y. 1955) (refusing to enter a protective order requiring the plaintiff to waive any potential personal injury liability as a prerequisite of an inspection because any duty owed to the plaintiff during the inspection, "whatever it is, is fixed by law" and the court did not need to prejudge that duty).

Conversely, such costs are reasonable for a large publicly traded corporation like Sirius. Sirius has made the business decision to collect and use the Call Recipient Contact Information in its business practices, and has accepted the risks that go along with using such data. It can, and presumably has, taken appropriate steps to mitigate its financial liability, for example, by procuring appropriate insurance policies to cover data theft, and by taking proper reserves to pay for the expenses it may incur in the event of a data theft.

Asking individual Data Recipients to take on such potential liability will have a direct effect on Plaintiff's ability to prosecute this action. Likewise, asking an expert or a vendor to personally agree to the indemnification Sirius will deter their willingness to work with Plaintiff, thereby limiting Plaintiff's choice of experts and vendors. As noted, at least one of the vendors identified by Plaintiff already refused to host the data expressly because of the liability created by the indemnification clause. It will also force Plaintiff's counsel into the unenviable position of taking on significant potential personal liability and/or insurance costs in order to fulfill their duty to represent their client. As such, Sirius' indemnification provisions would impose "hardship and prejudice" on Plaintiff, which outweighs the benefits to Sirius XM. *See Merial Ltd.* 2010 WL 11534378, at *2.

Even though courts in the Fifth Circuit have not examined whether a party like Sirius is entitled to indemnification as a requirement for producing information required under the Federal Rules, courts outside the circuit have refused to grant protective orders that include indemnification requirements in other contexts. For example, courts have refused to require indemnification or waiver of liability prior to physical inspections under Rule 34. *E.g., U.S. v. Bunker Hill Co.*, 417 F. Supp. 332, 333 (D. Idaho 1976) (refusing to enter a protective order that required the U.S. as plaintiff to agree to indemnify the defendant for any damage caused by the

government's inspection of defendant's land); Handbk. Fed. Civ. Disc. & Disclosure § 9:12 (4th ed.) ("The court will not condition an order for inspection of property upon the execution by the inspecting party of an indemnification agreement, in which the responding party seeks indemnification against any claims arising from the inspection or for damages to its property resulting from the inspection."). Similarly, courts have refused to require non-governmental parties to agree to indemnify government entities from the expense of defending against public record requests for confidential documents produced during litigation. *E.g.*, *Traylor Bros., Inc. v. San Diego Unified Port Dist.,* No. CIV. 08-1019-L WVG, 2011 WL 666885, at *3 (S.D. Cal. Feb. 16, 2011) (holding that the defendant government entity's demand that plaintiff "agree to defend and indemnify it for costs and expenses of responding to a [California Public Records Act] request does not have merit" because the government had "not presented to the Court any authority that would support such a request").

Plaintiff's counsel asked Sirius to justify its demand for indemnification. Sirius provided several responses, none of which are availing here. (Ex. 7.) First, Sirius asserted that it asks for "an indemnification from anyone to whom it releases personally identifiable information in the ordinary course of business." (*Id.*) However, a litigation is not the "ordinary course of business." Plaintiff is not asking for this information as part of a two-way business transaction, Plaintiff has a right to this information under the Federal Rules, a right that should not be unduly burdened as Sirius now demands.

Second, Sirius claimed that "many of the OEMs with which Sirius has relationships require the appropriate protection of consumer data." (Ex. 7.) As noted above, Sirius has refused to identify those OEM's or the contractual provisions requiring such protection, and such contractual

protections should not inhibit Plaintiff's ability to prosecute his claims and those of the other class members. *Nvision Biomedical Techs., LLC,* 2016 WL 8285637 at *2.

Third, Sirius argued that the indemnification would "encourage and incentivize plaintiff's counsel and their vendor to adopt the appropriate level of protection." (Ex. 7.) Plaintiff agrees that a standard protective order, carrying the weight of this Court behind it, is appropriate to protect the Call Recipient Contact Information. Plaintiff and his counsel require no additional encouragement or incentive to abide by any order of this Court and will of course ensure Sirius' information is protected as per any order of this Court.

Fourth, Sirius asserted that "[s]ecurity breaches and data hacks unfortunately are a feature of today's world, and again this is risk allocation between Sirius and its shareholders, on the one hand, and the plaintiff (and his counsel) who chose to sue Sirius XM, on the other." (Ex. 7.) Nevertheless, Sirius placed phone calls to Plaintiff after he placed his name and number on both the National and Sirius' internal do-not-call lists. Plaintiff is now asserting his rights, and those of others similarly situated, under the TCPA to prevent such calls. Sirius' statement indicates that it believes that if Plaintiff or his counsel are unwilling to take on potentially crippling personal liability, then they should not be allowed to "choose to sue Sirius XM" in order to enforce Plaintiff's rights. However, justice is not only available to those that have the resources of a publicly traded corporation like Sirius, justice is available to all. Sirius should not be allowed to use its indemnification demand as a tool to avoid prosecution by anyone not wealthy enough to take on such personal liability.

CONCLUSION

For the foregoing reasons, Plaintiff respectfully requests that the Court overrule Sirius's objections and order a fully responsive production of the call logs, and enter a protective order in the form attached as Exhibit 9 to the Ellzey Affidavit, without the Data Security Acknowledgment.

Respectfully Submitted,

/s/ Jarrett L. Ellzey
W. Craft Hughes
craft@hughesellzey.com
Jarrett L. Ellzey
jarrett@hughesellzey.com
HUGHES ELLZEY, LLP
2700 Post Oak Blvd., Suite 1120
Houston, TX 77056
Phone (713) 554-2377
Facsimile (888) 995-3335

Mark A. Alexander
mark@markalexanderlaw.com
Mark A. Alexander P.C.
5080 Spectrum, Suite 850E
Addison, Texas 75001
Tel: 972.364.9700
Fax: 972. 239.2244

Henry A. Turner*
Turner Law Offices, LLC
403 W. Ponce de Leon Avenue
Suite 207
Decatur, Georgia 30030
Tel: (404) 378-6274
hturner@tloffices.com

Aaron Siri*
Siri & Glimstad LLP
200 Park Avenue, 17th Floor
New York, New York 10166
Tel: (212) 532-1091
aaron@sirillp.com

Douglas M. Werman*
Werman Salas P.C.
77 West Washington, Suite 1402
Chicago, Illinois 60602
Tel: (312) 419-1008
dwerman@flsalaw.com

CERTIFICATE OF CONFERENCE

I certify a copy of the foregoing document was electronically filed with the Clerk of this Court using the CM/ECF system in accordance with the protocols for e-filing in the United States District Court for the Northern District of Texas, Dallas Division, on March 7, 2018, and will be served on all counsel of record who have consented to electronic notification *via* CM/ECF.

/s/ Jarrett L. Ellzey
Jarrett L. Ellzey

CERTIFICATE OF CONFERENCE

I certify that on multiple occasions during the months of December, 2017, and January 2018, Plaintiffs conferred with counsel for Defendant regarding the substance of a protective order and Defendant's deficient document production. Then parties have reached an impasse regarding the content of a protective order and Defendant's outstanding discovery responses; therefore, Plaintiff, has moved for the relief requested in this motion.

/s/ Jarrett L. Ellzey
Jarrett L. Ellzey